10 EVIDENCE INVOLVING IMAGES

10.1 Purpose

This document contains the procedures for the proper collection and preservation of digital forensic evidence. Computer search software or graphics software can be used to view images on any device that contains or stores images. This procedure can be used as a stand-alone analysis process, or may be the precursor to further forensic analysis.

10.2 Scope

This procedure applies to all digital still cameras or digital video cameras with downloading capabilities. This can include, but not limited to, digital storage media, thumb drives flash cards, hard drives, etc.

10.3 Materials - Equipment (Hardware/Software)

The following equipment and materials may be utilized:

- Computer hardware and software
- Camera
- Cleaning materials
- Imaged hard drive
- Cell phones
- Other image storage devices
- Approved graphics viewer software
- Standard computer tools
- Forensic imaging hardware and software
- NOTE: Some digital cameras may preserve data only so long as power is provided; therefore, care should be taken to examine digital cameras as soon after submission as possible to reduce the potential of data loss.

10.4 Limitations

None for this procedure

10.5 Safety

None for this procedure

10.6 Procedures

10.6.1 Ensure preliminary examination has been conducted.

10.6.2 Inspect submitted evidence and record necessary information such as make, model, serial number and external markings as applicable. This information is to be recorded in the case file notes and may be in the form of a photograph or photo copy.

10.6.3 Obtain applicable User's Manual, if necessary.

10.6.4 Conduct physical inspection for foreign substance(s); if present, the item may require cleaning.

    10.6.4.1 Prior to cleaning, verify that the item does not require any additional analysis such as latent prints, forensic biology, etc.

10.6.5 Run a file search to locate files with graphic or movie file extensions (i.e. jpg, gif, bmp, mov, mpg, avi, etc.).

10.6.6   Examine files recovered for data useful to the case.

10.6.7   Indicate if any files found have useable information.

10.6.8   Produce the results in a form that best represents the results (i.e. CD, DVD, hard copy, etc.).

10.7   References

Owner's Manuals, User's Manuals and appropriate software manuals should be referenced for equipment and operating instructions.

Blitzer, Herbert L., and Jack Jacobia. Forensic Digital Imaging and Photography. San Diego: Academic Press, 2002.

Damjanovski, Vlado. CCTV Networking and Digital Technology. 2nd ed. Amsterdam: Elsevier Butterworth - Heinemann, 2005.

Davies, Adrian, and Phil Fennessy. Digital Imaging for Photographers. 4th ed. Oxford: Focal Press, 2001.

Inglis, Andrew F. and Arch C. Luther. Video Engineering. 2nd ed. New York: McGraw-Hill, 1996.

Kruse, Warren G., and Jay G. Heiser. Computer Forensics Incident Response Essentials. Boston: Addison-Wesley, 2002.

Madisetti, Vijay K., and Douglas B. Williams, eds. The Digital Signal Processing Handbook. N.p.: CRC Press LLC, 1998.

Matchett, Alan R. CCTV for Security Professionals. Amsterdam: Butterworth – Heinemann, 2003.

Solari, Stephen J., Digital Video and Audio Compression. New York: McGraw-Hill, 1997.

Utz, Peter. Today's Video. 4th ed. Jefferson, NC: McFarland and Company, Inc., 2006.

Whitaker, Jerry, and Blair Benson. Standard Handbook of Video and Television Engineering. 3rd ed. New York: McGraw-Hill, 2000.

Electronic Crime Scene Investigation a Guide for First Responders. Washington, D.C.: U.S. Department of Justice, 2001.

Best Practices for Seizing Electronic Evidence a Pocket Guide for First Responders. 3rd ed. Washington, D.C.: U.S. Department of Homeland Security, United States Secret Service.

◆**End**